**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media
6. **Network security**
7. What types of physical security measures can be put in place?

Physical security measures include locks, alarms and surveillance systems however these as mentioned are all physical and hence can’t stop a virtual assault.

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

A strategy that could be applied to a password to prevent unauthorised access is to ensure through a password policy that it meets certain requirements to increase its strength such a; 8 digits or more, include non-alphabetical characters such as ?,/ ect, and having a day limit to how long the password can be used before expiring.

**Firewall**

1. Describe the nature of a firewall.

(in your own words can you send me a definition of nature in this usage, it isn’t totally clear to me)

A firewall is a server and software combination that filters information coming into the network, hence any packet deemed unauthorised is blocked.

1. What are the main purposes of firewalls and how are these purposes achieved?

The key purposes of a firewall is to block any packet of data that is flagged by the firewall as unwanted whether it be due to the protocol, ip or server address, domain name ect previously determined by the administrator of the computer, computer system in the program.

1. Why do firewalls use 2 separate NICs?

Firewalls use 2 separate NICs to prevent the system being circumnavigated as it then has to pass through the CPU of the server acting as a firewall.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware or Malicious software refers to threats such as spyware, adware, Trojan horses, worms and viruses, to help prevent these various strategies are put in motion these include a virus protection software being installed (most likely on the workstations) and kept up to date and a firewall implemented to name but a few.

**Encryption**

1. What is encryption?

Encryption is the process of translating the data being sent into a coded equivalent, that can only be read by an authorised user, therefor to read the encrypted file it is required that you have access to a secret key to decrypt it. Tho encrypt data becomes even more important when transmitting it over the internet or via radio waves.

1. Describe the nature of WPA or WPA2.

WPA (Wireless Protected Access) and WPA2 are security protocols to protect data transmitted over wireless LAN networks. This is in an attempt to provide equal security of that of a wired network.

1. What is encrypted data known as?

Encrypted data is known as a ciphertext where unencrypted data is known as plaintext.

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

The protocol used to secure financial transactions over the internet is the hypertext transfer protocol security or HTTPS, this acts as a secure protocol between a browser and the web server they are connecting to. This encrypts using 128 bit SSL (Secure Socket Layer) the transactions and authenticates them as they travel across the internet,

1. What is digital identification certificate technology based on?

The digital identification certificate technology is based on a trusted certificate authority such as Verisign Inc.

1. Describe the nature of Secure sockets layer (SSL) protocol.

SSL protocol is a cryptographic protocol providing secure connection to the internet, this verification occurs when a browser points to a secure domain, initiating a SSL ‘handshake’ that authenticates the webserver and the clients browser.

**Physical design of networks**

1. What is the role of a network diagram?

The main role of a network diagram is to schematically show the physical devices and communications lines present in the network, not that it doesn’t however correspond to the layout of the building as it prevents an unneeded lay of complication.